Identification of a given Boolean function with a mixed-state NMR quantum computer (Mathematical Study of Quantum Dynamical Systems and Its Application to Quantum Computer)

AUTHOR(S):

Ozawa, Hiroshi

数理解析研究所講究録 1350 巻 2004 年 10-25

10

Identification of a given Boolean function with a mixed-state NMR quantum computer

Hiroshi Ozawa
Information Technology Center, The University of Tokyo, Tokyo 113-0033, Japan
(小澤 宏 東京大学情報基盤センター)

Any given Boolean function $f(x) \in \{0,1\}$, $x = 1, \ldots, 2^n - 1$, is identified with n queries to the oracle which evaluates f with an n-spin mixed-state nuclear magnetic resonance (NMR) quantum computer. This means that the database searching problem to find x for which $f(x) = 1$ is solved with an exponential speedup, compared to classical methods. The procedure is a physical implementation of the probabilistic ensemble computer model, where the uniformly random input is realized by the mixed state of superpositions, to which function f is efficiently applied using quantum parallelism, and the exact probability of the output is certified by the ensemble averaging.

1. Introduction

A quantum computer [1,2] uses a collection of coupled two-state quantum systems as quantum bits (qubits), and executes computation by a sequence of unitary transformations on them; the result is obtained by measuring the final state (of a subset) of the qubits. Quantum computing [3] is exciting because quantum computers could solve some problems exponentially faster than by the best known classical methods. The algorithm proposed by Deutsch and Jozsa [1,4] was the first explicit example of a computational task which gained such a speedup, where an oracle (a black box) was used for function evaluation. This speedup was experimentally demonstrated with a quantum computer which employed nuclear magnetic resonance (NMR) spectroscopy [5,6]. [In the oracle models, the efficiency of computation (the speedup) is analyzed by the number of invocations (queries) to the oracle.] Another example of quantum algorithms to use the oracle was proposed by Grover [7,8] for database searching. The problem is: "for a given unstructured Boolean function $f(x) \in \{0,1\}$, $x = 0, \ldots, N-1$, find x such that $f(x) = 1$," and the Grover's algorithm solves this problem with $O(\sqrt{N})$ queries to the oracle which evaluates f. It is apparent that classically we require $O(N)$ evaluations of f, and therefore quantum effects provide a square-root speedup for this problem.

In these algorithms, the oracle to evaluate the given function f is a unitary transformation called f-controlled-NOT [1], which is defined by

$$U_f : \ |x\rangle|y\rangle \longmapsto |x\rangle|y \oplus f(x)\rangle \, . \tag{1}$$

When $|y\rangle$ is a one-qubit superposition state $(|0\rangle - |1\rangle)/\sqrt{2}$, this transformation gives

$$|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{U_f} (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} , \tag{2}$$

meaning that U_f can equivalently be defined [9] by

$$U_f : \ |x\rangle \longmapsto (-1)^{f(x)}|x\rangle \,. \tag{3}$$

Geometrical interpretation of the Grover's algorithm is as follows [10]. Assume that among the $N = 2^n$ equally weighted superposition states $|x\rangle$ of the initial state $|X\rangle$,

$$|X\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \,, \tag{4}$$

t states are the targets $[f(x) = 1]$, and others are not $[f(x) = 0]$:

$$|X_0\rangle = \frac{1}{\sqrt{N-t}} \sum_{x}^{(N-t)} |x\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{for non-target } |x\rangle \,, \tag{5}$$

$$|X_1\rangle = \frac{1}{\sqrt{t}} \sum_{x}^{(t)} |x\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{for target } |x\rangle \,. \tag{6}$$

Then we have

$$|X\rangle = \begin{bmatrix} \cos\theta \\ \sin\theta \end{bmatrix}, \quad \text{where} \quad \cos\theta = \sqrt{1 - \frac{t}{N}}, \quad \sin\theta = \sqrt{\frac{t}{N}} \,. \tag{7}$$

The Grover's kernel G is defined by $G = D\,U_f$, where U_f executes an "inversion of the targets," and D executes an "inversion about the average" [8]:

$$U_f = 1 - 2|X_1\rangle\langle X_1| = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad D = 2|X\rangle\langle X| - 1 = \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix}. \tag{8}$$

Notice that U_f of Eq. (8) is equivalent to that of Eq. (3) for the present case. With quantum computers, transformation D, as well as U_f, can be applied to the superposition states such as $|X_0\rangle$ and $|X_1\rangle$; D is implemented by a phase-shift operation sandwiched by the Hadamard transformations [8]. Then, using that

$$G = D\,U_f = \begin{bmatrix} \cos 2\theta & -\sin 2\theta \\ \sin 2\theta & \cos 2\theta \end{bmatrix}, \quad G^k = \begin{bmatrix} \cos 2k\theta & -\sin 2k\theta \\ \sin 2k\theta & \cos 2k\theta \end{bmatrix}, \tag{9}$$

we obtain

$$G^k|X\rangle = \begin{bmatrix} \cos(2k+1)\theta \\ \sin(2k+1)\theta \end{bmatrix}. \tag{10}$$

This equation tells that, when $1 \leq t \ll N$ (i.e. $0 < \sin\theta \ll 1$), $k \approx (\pi/4)\sqrt{N/t}$ iterations of G, and therefore the same number of evaluations of f by U_f, brings the initial state $|X\rangle$ to the target state $|X_1\rangle$. If we observe this state, we obtain one of the target values x, and the searching problem is solved. The square-root speedup obtained by this algorithm is optimal [11]. We need a related procedure of quantum counting, which uses quantum Fourier transformation [12], to know the number of the targets, t.

The Grover's algorithm outlined above is bases on the assumption that amplitude amplification to obtain $|X_1\rangle$ is necessary in order to obtain the target values x with

certainty. This situation is illustrated as follows. If we observe, for example, a one-qubit superposition state

$$|\psi\rangle = |c_0|e^{\phi_0}|0\rangle + |c_1|e^{\phi_1}|1\rangle\,, \quad |c_0|^2 + |c_1|^2 = 1\,, \tag{11}$$

we obtain either of the eigenvalues of the eigenstates $|0\rangle$ and $|1\rangle$, with the respective probability $|c_0|^2$ or $|c_1|^2$; if either state is not the target, we cannot obtain the target value with certainty. However, in NMR quantum computer experiments where bulk number of molecules are used as an ensemble of spin (qubit) systems, the situation is different. The magnetization we observe along the external magnetic field (the z axis) for a spin ensemble is proportional to the expectation value $\langle I_z\rangle$ of the spin angular momentum I_z [13], and, using the density operator $\rho = |\psi\rangle\langle\psi|$ for the pure ensemble of Eq. (11), $\langle I_z\rangle$ is calculated (see Sect. 2) as

$$\langle I_z\rangle = \mathrm{Tr}[\rho I_z] = \frac{1}{2}(|c_0|^2 - |c_1|^2)\,. \tag{12}$$

This is the weighted average of the eigenvalues $1/2$ and $-1/2$, i.e. the eigenvalues of the states $|0\rangle$ and $|1\rangle$ for the spin operator I_z. Similarly, we can observe the magnetization along the x axis, which is proportional to

$$\langle I_x\rangle = \mathrm{Tr}[\rho I_x] = |c_0||c_1|\cos(\phi_1 - \phi_0)\,. \tag{13}$$

This means that observation of a superposition state for an ensemble gives a deterministic result of the exact probability. Therefore, in NMR, amplitude amplification can be unnecessary for the database searching, and we have a prospect that we can solve this problem with less number of evaluations of f than in the Grover's algorithm.

In this work, we will show that, with an n-qubit mixed-state NMR quantum computer, we can identify any given unstructured Boolean function $f(x) \in \{0,1\}$, $x = 1,\ldots,2^n-1$, with n queries to the f-controlled-NOT oracle U_f defined by Eq. (3). [We assume $f(0) = 0$.] To solve this problem by classical methods we need $O(2^n)$ evaluations, and therefore we obtain an exponential speedup. When this procedure is applied to the database searching problem described above, it is also solved with an exponential (rather than a square-root) speedup, where the number of the targets t can be arbitrary ($0 \le t < 2^n$), and t is automatically counted without resorting to a related procedure.

Our NMR procedure of the Boolean function identification [Sect. 2] is to apply an f-controlled-NOT transformation U_f of the given function f to a mixed superposition state ρ_{ini}, and observe the NMR spectrum of the resulting state; the spectrum is obtained by a slightly modified version of the conventional pulsed-Fourier transformation technique [13]. This procedure is different from some other NMR quantum procedures in that we use mixed states, rather than "effective pure (pseudo-pure) states" [5,6]. The speedup is exponential, because, when the problem size is 2^n, we obtain the spectrum which has the one-to-one correspondence to the given function f in n experiments (in practice, in a single experiment) [Sects. 2.1–2.3], and we can implement any U_f in NMR [Sect. 3]. Although this speedup is basically provided by the power of the probabilistic ensemble computation, we need quantum parallelism [1], which is a major origin of the power of quantum computation, in implementing such computer model, and our procedure makes use of both the ensemble and the quantum nature of spins [Sect. 4].

2. NMR procedure

In this work, we denote the eigenstates of a spin-1/2 by

$$|\uparrow_z\rangle = |0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad \text{and} \quad |\downarrow_z\rangle = |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \tag{14}$$

where z is the direction of the quantization axis, i.e. the external magnetic field applied to the spin. The bases of single-spin operators in the Cartesian coordinate are given by

$$\mathbf{1} \quad \text{and} \quad I_\alpha = \frac{1}{2}\sigma_\alpha, \quad \alpha = x, y, z, \tag{15}$$

where $\mathbf{1}$ is a 2×2 unit matrix, and σ_α are the Pauli matrices:

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{16}$$

We express the density operator of a spin system in the product operator formalism [13] of single-spin operators.

We assume to use an NMR quantum computer, where of the order of Avogadro's number of identical molecules in liquid state and at room temperature are placed in an external static magnetic field along the z axis; each molecule forms a homonuclear n-spin system, and spins of different molecules have no interaction. Such sample makes an ensemble of n-spin systems. The density operator ρ of the total spin-system ensemble, at thermal equilibrium, is described by the Boltzmann distribution,

$$\rho = \frac{1}{Z} e^{-\mathcal{H}/kT}. \tag{17}$$

Here, $\mathcal{H}$ is the n-spin Hamiltonian

$$\frac{\mathcal{H}}{\hbar} = -\sum_{i=1}^{n} \omega_0^i I_z^i + \sum_{i>j}^{n} 2\pi J_{ij} I_z^i I_z^j, \tag{18}$$

where ω_0^i is the Larmor precession frequency of the ith spin, and J_{ij} is the spin-spin coupling constant between the ith and jth spins. We assume that all spins have different Larmor frequencies (chemical shifts), and the spins are fully coupled for all spin pairs. We further assume that the spin-spin coupling constants are much smaller that the chemical-shift differences, i.e. $|J_{ij}| \ll |\omega_0^k - \omega_0^l|$. We choose such molecule for our NMR quantum computer. Then, in the high temperature limit, i.e. at room temperature, the density operator of Eq. (17) is given, to a good approximation, by

$$\rho = \frac{1}{Z}(\mathbf{1} + \frac{\hbar\omega_0}{kT} \sum_{i=1}^{n} I_z^i), \tag{19}$$

where $\hbar\omega_0/kT \approx 10^{-5}$ when $\omega_0 = 2\pi \times 400$ MHz, which is the resonance frequency of protons at 9.4 T filed. This means that the energy levels of spins are almost equally populated, and the phases of spins are random. The magnetization we observe in NMR, at thermal equilibrium and at room temperature, is what corresponds to the magnetization that would be observed when a 10^{-5} portion of the total spins was polarized along the z axis. This state is described by the mixed-state density operator

$$\rho_{eq}^{(n)} = \sum_{i=1}^{n} I_z^i, \tag{20}$$

where we omitted the proportionality constant. The density matrix of Eq. (20), which corresponds to the traceless part of the density matrix of the total spin-system ensemble, is called the deviation density matrix [5] in the NMR terminology. We treat this density operator throughout this work.

In the Grover's algorithm, the initial state $|X\rangle$ of calculation is the Hadamard transform of an n-qubit pure state $|00\cdots0\rangle$; the Hadamard transformation H is defined by

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{21}$$

In NMR, several methods have been proposed to prepare, from the thermal equilibrium state of Eq. (20), "effective pure states" [5,6] which transform identically to pure states. For example, by the method of spatial labeling [6,14], "effective pure $|00\cdots0\rangle$ states" are known to be prepared for any number of spins [15]. In this work, however, we will skip preparing such state, and use, as our initial state of calculation, the direct Hadamard transform of the thermal equilibrium state. When we apply the Hadamard transformation to each term on the right-hand side of Eq. (20), we obtain the density operator $\rho_{ini}^{(n)}$ of our initial state,

$$\rho_{ini}^{(n)} = \sum_{i=1}^{n} I_x^i . \tag{22}$$

Experimentally, we obtain this spin state by applying a non-selective $(-\pi/2)_y(I^i)$ pulse (see Sect. 3), which implements a simplified version of the Hadamard transformation, to all spins of our total spin-system ensemble. The state of Eq. (22) is also mixed, in contrast to the pure state of $|X\rangle$.

When the size of the Boolean function identification problem is $N = 2^n$, as in Eq. (4), we define the given function f by

$$f_{a_0\ldots a_{N-1}}(x) = a_x\,, \qquad x = 0,\ldots,N-1\,, \tag{23}$$

where

$$a_1,\ldots,a_{N-1} \in \{0,1\}\,, \tag{24}$$

and we assume

$$a_0 = 0\,. \tag{25}$$

This means that we have 2^{N-1} different functions f. Then, by the definition of Eq. (3), the f-controlled-NOT transformation U_f for $f_{a_0\ldots a_{N-1}}$ is given by

$$U_{f_{a_0\ldots a_{N-1}}} = \sum_{x=0}^{N-1} (-1)^{a_x} |x\rangle\langle x|\,. \tag{26}$$

As briefly described above, our procedure to identify the given function $f_{a_0\ldots a_{N-1}}$ [Eq. (23)] by NMR is to apply an $U_{f_{a_0\ldots a_{N-1}}}$ transformation [Eq. (26)] to our initial state $\rho_{ini}^{(n)}$ [Eq. (22)], and observe the (frequency-domain) NMR spectrum of the resulting state. The spectrum is obtained as follows. If we neglect the decoherence (our

computation is assumed to be complete within the decoherence time), time evolution of the density operator ρ is given by the Liouville-von Neumann equation

$$\frac{d\rho}{dt} = i[\rho, \frac{\mathcal{H}}{\hbar}], \tag{27}$$

whose solution is

$$\rho(t) = e^{-i(\mathcal{H}/\hbar)t}\rho(0)e^{i(\mathcal{H}/\hbar)t}. \tag{28}$$

When we denote, by $\rho(0)$, the density operator of our spin system just after we applied $U_{f_{a_0\cdots a_{N-1}}}$ to $\rho_{ini}^{(n)}$, it evolves according to this equation, where $\mathcal{H}$ is the time-independent Hamiltonian given in Eq. (18). We observe the x component of the spin angular momentum of the ith spin, I_x^i, whose expectation value evolves according to

$$\langle I_x^i \rangle(t) = \mathrm{Tr}[\rho(t) I_x^i], \tag{29}$$

and collect the (time-domain) free induction decay (FID) signal M_x^i which is proportional to $\langle I_x^i \rangle(t)$. We finally Fourier transform M_x^i to obtain the NMR spectrum of the ith spin along x, which reflects information on $\rho(0)$, and therefore on $f_{a_0\ldots a_{N-1}}$.

2.1. Problem of size $N = 2^2$

We will first consider identifying a given Boollean function of size $N = 2^2$ with an NMR quantum computer of two-spin systems. We denote the first and second spins by I and S, respectively. The density operator (and its matrix) of our spin system at thermal equilibrium is given by

$$\rho_{eq}^{(2)} = I_z + S_z = \frac{1}{2}\begin{bmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{bmatrix}, \tag{30}$$

which, when the Hadamard transformation is applied to each spin, transforms to our initial state

$$\rho_{ini}^{(2)} = I_x + S_x = \frac{1}{2}\begin{bmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{bmatrix}. \tag{31}$$

When $n = 2$, we have eight different functions $f_{a_0a_1a_2a_3}$. For example, f_{0100} is defined by

$$f_{0100}(0) = 0, \quad f_{0100}(1) = 1, \quad f_{0100}(2) = 0, \quad f_{0100}(3) = 0, \tag{32}$$

and the f-controlled-NOT transformation U_f [Eq. (26)] for f_{0100} is

$$U_{f_{0100}} = |00\rangle\langle 00| - |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11| = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix}. \tag{33}$$

When we apply $U_{f_{0100}}$ to $\rho_{ini}^{(2)}$, we obtain ρ_{0100}:

$$\rho_{ini}^{(2)} \xrightarrow{U_{f_{0100}}} \rho_{0100} = \frac{1}{2}\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix} - \frac{1}{2}\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{bmatrix} = 2I_xS_z - 2I_zS_x\,. \tag{34}$$

For the general case of function $f_{a_0a_1a_2a_3}$, the f-controlled-NOT transformation given by

$$U_{f_{a_0a_1a_2a_3}} = \begin{bmatrix} (-1)^{a_0} & & & \\ & (-1)^{a_1} & & \\ & & (-1)^{a_2} & \\ & & & (-1)^{a_3} \end{bmatrix} \tag{35}$$

transforms each term I_x and S_x of Eq. (31) as follows:

$$I_x \xrightarrow{U_{f_{a_0a_1a_2a_3}}} (-1)^{a_0\oplus a_2} I_x\,(\frac{1}{2}\mathbf{1} + S_z) + (-1)^{a_1\oplus a_3} I_x\,(\frac{1}{2}\mathbf{1} - S_z)\,, \tag{36}$$

$$S_x \xrightarrow{U_{f_{a_0a_1a_2a_3}}} (-1)^{a_0\oplus a_1}(\frac{1}{2}\mathbf{1} + I_z)\,S_x + (-1)^{a_2\oplus a_3}(\frac{1}{2}\mathbf{1} - I_z)\,S_x\,. \tag{37}$$

Using these relations, we obtain the following density operators, $\rho_{a_0a_1a_2a_3}$, for the states after we apply $U_{f_{a_0a_1a_2a_3}}$ to $\rho_{ini}^{(2)}$:

$$\begin{aligned} &\rho_{0000} = I_x + S_x\,, \quad \rho_{0001} = 2I_xS_z + 2I_zS_x\,, \quad \rho_{0010} = -2I_xS_z + 2I_zS_x\,, \\ &\rho_{0011} = -I_x + S_x\,, \quad \rho_{0100} = 2I_xS_z - 2I_zS_x\,, \quad \rho_{0101} = I_x - S_x\,, \\ &\rho_{0110} = -I_x - S_x\,, \quad \rho_{0111} = -2I_xS_z - 2I_zS_x\,. \end{aligned} \tag{38}$$

We will next calculate time evolutions of two of the terms, I_x and $2I_xS_z$, which appear on the right-hand sides of these equations, due to the two-spin system Hamiltonian

$$\frac{\mathcal{H}}{\hbar} = -\omega_0^I I_z - \omega_0^S S_z + 2\pi J_{IS} I_z S_z\,. \tag{39}$$

We here use the following equations of spin operators in the exponential form [16]:

$$\exp[i\theta I_\alpha] = \cos\frac{\theta}{2}\mathbf{1} + 2i\sin\frac{\theta}{2}I_\alpha\,, \qquad \exp[i\theta I_zS_z] = \cos\frac{\theta}{4}\mathbf{1} + 4i\sin\frac{\theta}{4}I_zS_z\,; \tag{40}$$

these equations are derived from the definition of exponential operators, i.e. $\exp[iA] = \sum_{n=0}^{\infty}[(iA)^n/n!]$, and the relation $I_\alpha^2 = 1/4$, $\alpha = x, y, z$. Using Eq. (40) and the commutation relations $I_xI_y = -I_yI_x = (i/2)I_z$, etc., we obtain [13] $\exp[i\theta I_z]\,I_x \exp[-i\theta I_z] = I_x\cos\theta - I_y\sin\theta$, $\exp[-i\theta I_zS_z]\,I_x \exp[i\theta I_zS_z] = I_x\cos(\theta/2) + 2I_yS_z\sin(\theta/2)$, etc., and time evolutions of I_x and $2I_xS_z$ are calculated as follows:

$$\begin{aligned} I_x \xrightarrow{\exp[-i(\mathcal{H}/\hbar)t]} &(I_x\cos\omega_0^I t - I_y\sin\omega_0^I t)\cos\pi J_{IS}t \\ &+(2I_xS_z\sin\omega_0^I t + 2I_yS_z\cos\omega_0^I t)\sin\pi J_{IS}t\,, \end{aligned} \tag{41}$$

$$\begin{aligned} 2I_xS_z \xrightarrow{\exp[-i(\mathcal{H}/\hbar)t]} &(I_x\sin\omega_0^I t + I_y\cos\omega_0^I t)\sin\pi J_{IS}t \\ &+(2I_xS_z\cos\omega_0^I t - 2I_yS_z\sin\omega_0^I t)\cos\pi J_{IS}t\,. \end{aligned} \tag{42}$$

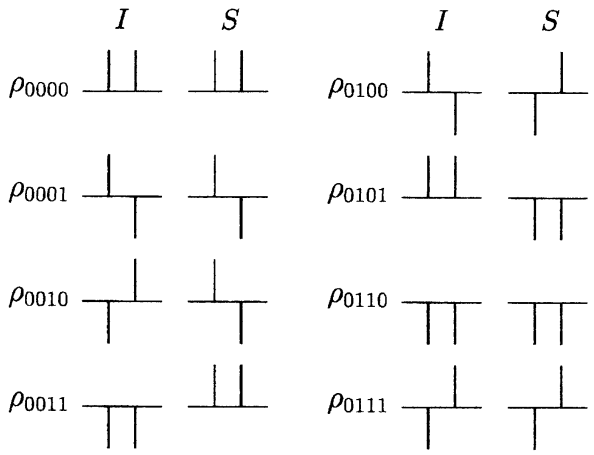

Figure 1. NMR spectra expected in identifying a given $N = 2^2$ Boolean function f using a two-spin system IS, where an f-controlled-NOT transformation U_f is applied to the Hadamard transform of the thermal equilibrium state, and the FID signal is collected and Fourier transformed. Left patterns show the I spectra, at the frequencies $\omega_0^I - \pi J_{IS}$ (left lines) and $\omega_0^I + \pi J_{IS}$ (right lines). Right patterns show the S spectra, at the frequencies $\omega_0^S - \pi J_{IS}$ (left lines) and $\omega_0^S + \pi J_{IS}$ (right lines).

As previously described, the collected FID signal M_x^I of spin I along x is proportional to the expectation value $\langle I_x \rangle(t)$ [Eq. (29)]. Using that only the first terms on the right-hand sides of Eqs. (41) and (42) give nonzero traces for $\mathrm{Tr}[\rho(t) I_x]$, M_x^I due to the two terms are calculated as

$$M_x^I(I_x) \propto \cos\omega_0^I t \cos\pi J_{IS} t = \frac{1}{2}\left[\cos(\omega_0^I - \pi J_{IS})t + \cos(\omega_0^I + \pi J_{IS})t\right], \tag{43}$$

$$M_x^I(2I_xS_z) \propto \sin\omega_0^I t \sin\pi J_{IS} t = \frac{1}{2}\left[\cos(\omega_0^I - \pi J_{IS})t - \cos(\omega_0^I + \pi J_{IS})t\right]. \tag{44}$$

These equations tell that, when we Fourier transform M_x^I, we obtain two upward spectral lines at the frequency positions $\omega_0^I - \pi J_{IS}$ and $\omega_0^I + \pi J_{IS}$ for $M_x^I(I_x)$, and an upward and a downward line at the same respective positions for $M_x^I(2I_xS_z)$.

With these and similar considerations for the S spectrum, i.e. $M_x^S(S_x)$ and $M_x^S(2I_zS_x)$, we see that the spectral patterns for the eight states whose density operators were given in Eq. (38) are as shown in Fig. 1. This figure clearly shows that, if we look at spectral patterns of I and S spins, we know which $U_{f_{a_0a_1a_2a_3}}$ was applied to $\rho_{ini}^{(2)}$, and the given function $f_{a_0a_1a_2a_3}$ is identified. Here, if we obtained the I and S spectra by separate experiments, we evaluated the function twice ($n = 2$). In practice, we obtain the I and S spectra in a single experiment, by collecting the mixed FID signal of the two spins and Fourier transforming it; in this case the function was evaluated only once. In both cases, we could identify the given Boollean function with an exponential speedup, compared to classical methods.

2.2. Problem of size $N = 2^3$

We will next consider solving the $N = 2^3$ problem with a three-spin NMR quantum computer. Here we denote the third spin by K. When we apply the f-controlled-NOT

transformation

$$U_{f_{a_0\cdots a_7}} = \begin{bmatrix} (-1)^{a_0} & & & \\ & (-1)^{a_1} & & \\ & & \ddots & \\ & & & (-1)^{a_7} \end{bmatrix} \tag{45}$$

to our initial state

$$\rho_{ini}^{(3)} = I_x + S_x + K_x\,, \tag{46}$$

each term on the right-hand side of Eq. (46) transforms as follows:

$$\begin{aligned} I_x \xrightarrow{U_{f_{a_0\cdots a_7}}} & (-1)^{a_0\oplus a_4} I_x\,(\tfrac{1}{2}\mathbf{1} + S_z)(\tfrac{1}{2}\mathbf{1} + K_z) + (-1)^{a_1\oplus a_5} I_x\,(\tfrac{1}{2}\mathbf{1} + S_z)(\tfrac{1}{2}\mathbf{1} - K_z) \\ & + (-1)^{a_2\oplus a_6} I_x\,(\tfrac{1}{2}\mathbf{1} - S_z)(\tfrac{1}{2}\mathbf{1} + K_z) + (-1)^{a_3\oplus a_7} I_x\,(\tfrac{1}{2}\mathbf{1} - S_z)(\tfrac{1}{2}\mathbf{1} - K_z)\,, \end{aligned} \tag{47}$$

$$\begin{aligned} S_x \xrightarrow{U_{f_{a_0\cdots a_7}}} & (-1)^{a_0\oplus a_2}(\tfrac{1}{2}\mathbf{1} + I_z)\, S_x\,(\tfrac{1}{2}\mathbf{1} + K_z) + (-1)^{a_1\oplus a_3}(\tfrac{1}{2}\mathbf{1} + I_z)\, S_x\,(\tfrac{1}{2}\mathbf{1} - K_z) \\ & + (-1)^{a_4\oplus a_6}(\tfrac{1}{2}\mathbf{1} - I_z)\, S_x\,(\tfrac{1}{2}\mathbf{1} + K_z) + (-1)^{a_5\oplus a_7}(\tfrac{1}{2}\mathbf{1} - I_z)\, S_x\,(\tfrac{1}{2}\mathbf{1} - K_z)\,, \end{aligned} \tag{48}$$

$$\begin{aligned} K_x \xrightarrow{U_{f_{a_0\cdots a_7}}} & (-1)^{a_0\oplus a_1}(\tfrac{1}{2}\mathbf{1} + I_z)(\tfrac{1}{2}\mathbf{1} + S_z)\, K_x + (-1)^{a_2\oplus a_3}(\tfrac{1}{2}\mathbf{1} + I_z)(\tfrac{1}{2}\mathbf{1} - S_z)\, K_x \\ & + (-1)^{a_4\oplus a_5}(\tfrac{1}{2}\mathbf{1} - I_z)(\tfrac{1}{2}\mathbf{1} + S_z)\, K_x + (-1)^{a_6\oplus a_7}(\tfrac{1}{2}\mathbf{1} - I_z)(\tfrac{1}{2}\mathbf{1} - S_z)\, K_x\,. \end{aligned} \tag{49}$$

Using these relations, we obtain the density operators $\rho_{a_0\cdots a_7}$ of the states whose spectra we are going to observe. Some of them are as follows:

$$\begin{aligned} \rho_{00000000} &= I_x + S_x + K_x\,, \\ \rho_{00000001} &= \frac{1}{2}(I_x + 2I_xS_z + 2I_xK_z - 4I_xS_zK_z + S_x + 2I_zS_x \\ &\quad +2S_xK_z - 4I_zS_xK_z + K_x + 2I_zK_x + 2S_zK_x - 4I_zS_zK_x)\,, \\ \rho_{00000010} &= \frac{1}{2}(I_x + 2I_xS_z - 2I_xK_z + 4I_xS_zK_z + S_x + 2I_zS_x \\ &\quad -2S_xK_z + 4I_zS_xK_z + K_x + 2I_zK_x + 2S_zK_x - 4I_zS_zK_x)\,, \\ \rho_{00000011} &= 2I_xS_z + 2I_zS_x + K_x\,, \\ \rho_{00000100} &= \frac{1}{2}(I_x - 2I_xS_z + 2I_xK_z + 4I_xS_zK_z + S_x + 2I_zS_x \\ &\quad +2S_xK_z - 4I_zS_xK_z + K_x + 2I_zK_x - 2S_zK_x + 4I_zS_zK_x)\,, \\ \rho_{00000101} &= 2I_xK_z + S_x + 2I_zK_x\,, \\ \rho_{00000110} &= 4I_xS_zK_z + 2I_zS_x + 2I_zK_x\,, \\ \rho_{00000111} &= \frac{1}{2}(-I_x + 2I_xS_z + 2I_xK_z + 4I_xS_zK_z + S_x + 2I_zS_x \\ &\quad -2S_xK_z + 4I_zS_xK_z + K_x + 2I_zK_x - 2S_zK_x + 4I_zS_zK_x)\,. \end{aligned} \tag{50}$$

Among terms which appear on the right-hand sides of these equations, we will here consider four of them, S_x, $2I_zS_x$, $2S_xK_z$, and $4I_zS_xK_z$, which decide the spectral pattern of spin S. The Hamiltonian of the three-spin system is

$$\frac{\mathcal{H}}{\hbar} = -\omega_0^I I_z - \omega_0^S S_z - \omega_0^K K_z + 2\pi J_{IS} I_z S_z + 2\pi J_{IK} I_z K_z + 2\pi J_{SK} S_z K_z\,, \tag{51}$$

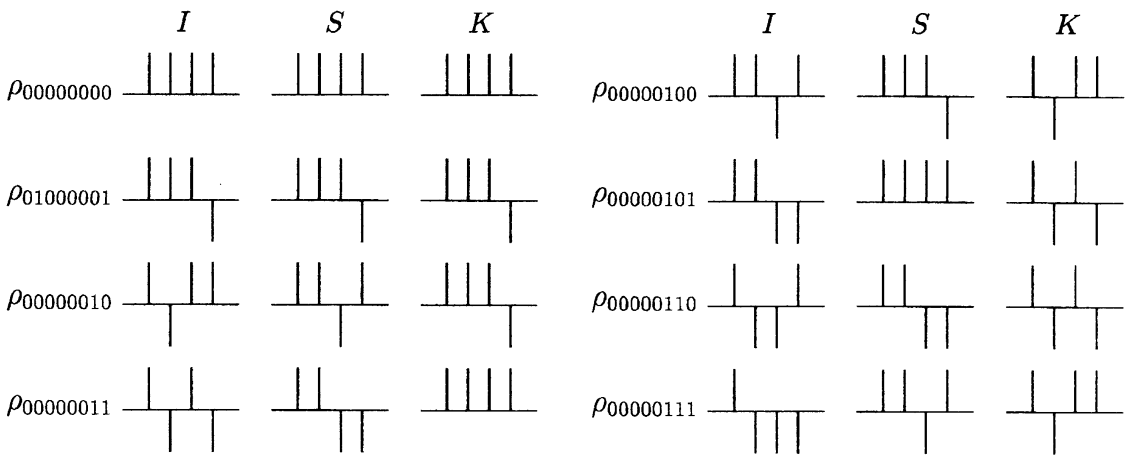

Figure 2. Some examples of the NMR spectra expected in identifying a given $N = 2^3$ Boolean function using a three-spin system ISK. Middle patterns show the S spectra, at the frequencies $\omega_0^S - \pi J_{IS} - \pi J_{SK}$, $\omega_0^S - \pi J_{IS} + \pi J_{SK}$, $\omega_0^S + \pi J_{IS} - \pi J_{SK}$, and $\omega_0^S + \pi J_{IS} + \pi J_{SK}$ (from left to right). Left (right) patterns show the I (K) spectra, at the frequencies $\omega_0^I - \pi J_{IK} - \pi J_{IS}$ ($\omega_0^K - \pi J_{SK} - \pi J_{IK}$), etc.

and, using Eq. (40), etc., time evolution of S_x, for example, due to the Hamiltonian is calculated as

$$\begin{aligned} S_x \xrightarrow{\exp[-i(\mathcal{H}/\hbar)t]} & (S_x \cos\omega^S t - S_y \sin\omega^S t)\cos\pi J_{IS}t \cos\pi J_{SK}t \\ & +2K_z(S_x \sin\omega^S t + S_y \cos\omega^S t)\cos\pi J_{IS}t \sin\pi J_{SK}t \\ & +2I_z(S_x \sin\omega^S t + S_y \cos\omega^S t)\sin\pi J_{IS}t \cos\pi J_{SK}t \\ & -4I_zK_z(S_x \cos\omega^S t - S_y \sin\omega^S t)\sin\pi J_{IS}t \sin\pi J_{SK}t\,. \end{aligned} \tag{52}$$

Therefore, when we collect the FID signal M_x^S of spin S along the x axis, the contribution from this term to M_x^S is given by

$$M_x^S(S_x) \propto \cos\omega_0^S t \cos\pi J_{IS}t \cos\pi J_{SK}t\,. \tag{53}$$

Similarly, the contributions from the other three terms, $2I_zS_x$, $2S_xK_z$, and $4I_zS_xK_z$, to M_x^S are calculated as

$$M_x^S(2I_zS_x) \propto \sin\omega_0^S t \sin\pi J_{IS}t \cos\pi J_{SK}t\,, \tag{54}$$

$$M_x^S(2S_xK_z) \propto \sin\omega_0^S t \cos\pi J_{IS}t \sin\pi J_{SK}t\,, \tag{55}$$

$$M_x^S(4I_zS_xK_z) \propto -\cos\omega_0^S t \sin\pi J_{IS}t \sin\pi J_{SK}t\,. \tag{56}$$

These equations, when modified as in Eqs. (43) and (44), tell that, when we Fourier transform the FID signal M_x^S, we obtain a quartet of spectral lines of spin S, at the frequency positions $\omega_0^S - \pi J_{IS} - \pi J_{SK}$, $\omega_0^S - \pi J_{IS} + \pi J_{SK}$, $\omega_0^S + \pi J_{IS} - \pi J_{SK}$, and $\omega_0^S + \pi J_{IS} + \pi J_{SK}$, whose patterns are $(+,+,+,+)$ for $M_x^S(S_x)$, $(+,+,-,-)$ for $M_x^S(2I_zS_x)$, $(+,-,+,-)$ for $M_x^S(2S_xK_z)$, and $(+,-,-,+)$ for $M_x^S(4I_zS_xK_z)$, where $+$ and $-$ denote an upward and a downward spectral line, respectively. It should be apparent that similar results are also obtained for the spectra of I and K spins. In Fig. 2 are shown the

spectral patterns of I, S, and K spins for the states whose density operators were given in Eq. (50).

The experimental procedure to determine the values of $a_1, \ldots, a_7$ is as follows. (We assumed $a_0 = 0$.) As an example, let us consider the case we observed an S spectrum of a pattern $(+,+,-,+)$; see the middle spectra of $\rho_{00000010}$ and $\rho_{00000111}$ in Fig. 2. This pattern occurs only when the four contributions to the spectrum described above are positive for $(+,+,+,+)$, $(+,+,-,-)$, and $(+,-,-,+)$, and negative for $(+,-,+,-)$. This means that

$$\begin{aligned}
&(-1)^{a_0 \oplus a_2} + (-1)^{a_1 \oplus a_3} + (-1)^{a_4 \oplus a_6} + (-1)^{a_5 \oplus a_7} = 2\,, \\
&(-1)^{a_0 \oplus a_2} + (-1)^{a_1 \oplus a_3} - (-1)^{a_4 \oplus a_6} - (-1)^{a_5 \oplus a_7} = 2\,, \\
&(-1)^{a_0 \oplus a_2} - (-1)^{a_1 \oplus a_3} + (-1)^{a_4 \oplus a_6} - (-1)^{a_5 \oplus a_7} = -2\,, \\
&(-1)^{a_0 \oplus a_2} - (-1)^{a_1 \oplus a_3} - (-1)^{a_4 \oplus a_6} + (-1)^{a_5 \oplus a_7} = 2
\end{aligned} \tag{57}$$

in Eq. (48), and these equations lead to

$$a_0 \oplus a_2 = 0\,, \quad a_1 \oplus a_3 = 0\,, \quad a_4 \oplus a_6 = 1\,, \quad a_5 \oplus a_7 = 0\,. \tag{58}$$

Patterns of the S spectrum have 16 variations, and by the procedure described here, we can identify whether each of $a_0 \oplus a_2$, $a_1 \oplus a_3$, $a_4 \oplus a_6$, and $a_5 \oplus a_7$ is 0 or 1. Similarly, observation of the I spectrum gives information whether each of $a_0 \oplus a_4$, $a_1 \oplus a_5$, $a_2 \oplus a_6$, and $a_3 \oplus a_7$ is 0 or 1, and observation of the K spectrum gives information whether each of $a_0 \oplus a_1$, $a_2 \oplus a_3$, $a_4 \oplus a_5$, and $a_6 \oplus a_7$ is 0 or 1. Therefore, by using a selection of seven equations from these, we can uniquely determine each value of $a_1, \ldots, a_7$ in $\{0, 1\}$, and the given function $f_{a_0 \ldots a_7}$ is identified.

2.3. Problem of any size $N = 2^n$

The procedure described above can be extended to any problem size. To solve a problem of size $N = 2^n$, we use an NMR computer of n-spin systems. We apply an f-controlled-NOT transformation $U_{f_{a_0 \ldots a_{N-1}}}$ of the given function $f_{a_0 \ldots a_{N-1}}$ to the Hadamard transform of the n-spin thermal equilibrium state, and obtain the NMR spectrum by collecting and Fourier transforming the FID signal. This type of spins gives n spectra, each of which is made up of 2^{n-1} spectral lines. [The intensity (or signal-to-noise ratio) of each spectral line scales by $1/2^{n-1}$. This magnitude of scaling also takes place in other NMR quantum procedures to use "effective pure states" [5,6].] By observing the spectral patterns of all spins, we obtain $2^{n-1}n$ equations on a_x, and we can determine $2^n - 1$ values of $a_1, \ldots, a_{N-1}$. Since this procedure is executed in n experiments (or, in practice, in a single experiment, as described previously), we can solve the problem to identify any given Boolean function of any size with an exponential speedup, compared to classical methods.

3. Implementation

We will next show that any f-controlled-NOT transformation $U_{f_{a_0 \ldots a_{N-1}}}$ can be implemented in NMR. We here calculate, using Eqs. (15), (16), and (40), the matrix representation of spin exponential operators. Some of the results are as follows:

$$\exp[\pm i \frac{\pi}{2} I_z] = \frac{1 \pm i}{\sqrt{2}} \begin{bmatrix} 1 & \\ & \mp i \end{bmatrix}\,,$$

$$\exp[\pm i\pi I_z S_z] = \frac{1 \pm i}{\sqrt{2}} \begin{bmatrix} 1 & & & \\ & \mp i & & \\ & & \mp i & \\ & & & 1 \end{bmatrix}, \qquad \exp[\pm i2\pi I_z S_z] = \pm i \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{bmatrix}. \tag{59}$$

The f-controlled-NOT transformations U_f are then expressed by the products of the spin exponential operators; for example,

$$U_{f_{0100}} = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{bmatrix} = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & -i & \\ & & & -i \end{bmatrix} \begin{bmatrix} 1 & & & \\ & i & & \\ & & 1 & \\ & & & i \end{bmatrix} \begin{bmatrix} 1 & & & \\ & i & & \\ & & i & \\ & & & 1 \end{bmatrix} = \exp[i\pi(\tfrac{1}{2} + I_z)(\tfrac{1}{2} - S_z)],$$

$$U_{f_{0110}} = \begin{bmatrix} 1 & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{bmatrix} = \exp[i\pi(\tfrac{1}{2} - 2I_z S_z)]. \tag{60}$$

The general forms of U_f for the cases of $n = 2$ and 3 are calculated [17] as

$$\begin{aligned} U_{f_{a_0a_1a_2a_3}} &= \exp\left[i\frac{\pi}{2}[1 - (-1)^{a_0}](\frac{1}{2} + I_z)(\frac{1}{2} + S_z)\right] \\ &\quad \times \exp\left[i\frac{\pi}{2}[1 - (-1)^{a_1}](\frac{1}{2} + I_z)(\frac{1}{2} - S_z)\right] \exp\left[i\frac{\pi}{2}[1 - (-1)^{a_2}](\frac{1}{2} - I_z)(\frac{1}{2} + S_z)\right] \\ &\quad \times \exp\left[i\frac{\pi}{2}[1 - (-1)^{a_3}](\frac{1}{2} - I_z)(\frac{1}{2} - S_z)\right], \end{aligned} \tag{61}$$

$$\begin{aligned} U_{f_{a_0 \cdots a_7}} &= \exp\left[i\frac{\pi}{2}[1 - (-1)^{a_0}](\frac{1}{2} + I_z)(\frac{1}{2} + S_z)(\frac{1}{2} + K_z)\right] \\ &\quad \times \exp\left[i\frac{\pi}{2}[1 - (-1)^{a_1}](\frac{1}{2} + I_z)(\frac{1}{2} + S_z)(\frac{1}{2} - K_z)\right] \\ &\quad \times \cdots \times \exp\left[i\frac{\pi}{2}[1 - (-1)^{a_7}](\frac{1}{2} - I_z)(\frac{1}{2} - S_z)(\frac{1}{2} - K_z)\right]. \end{aligned} \tag{62}$$

Notice here that, for example, $\exp[i(\pi/2)I_z]$ is equivalent to

$$\exp[i\frac{\pi}{2}I_x] \exp[-i\frac{\pi}{2}I_y] \exp[-i\frac{\pi}{2}I_x], \tag{63}$$

and $\exp[-i2\pi I_z S_z K_z]$ is equivalent [18] to

$$\begin{aligned} &\exp[-i\frac{\pi}{2}I_x] \exp[-i\pi I_z K_z] \exp[-i\frac{\pi}{2}I_y] \exp[-i\pi I_z S_z] \\ &\qquad \times \exp[i\frac{\pi}{2}I_y] \exp[i\pi I_z K_z] \exp[i\frac{\pi}{2}I_x]. \end{aligned} \tag{64}$$

In this way we see that any f-controlled-NOT transformation $U_{f_{a_0 \cdots a_{N-1}}}$ of any size can be expressed by the product of spin exponential operators of the forms

$$\exp[i\theta I_x^i], \quad \exp[i\theta I_y^i], \quad \text{and} \quad \exp[-i\phi I_z^i I_z^j]. \tag{65}$$

In NMR, $\exp[i\theta I_\beta^i]$, $\beta = x, y$, is implemented by a selective pulse $(\theta)_\beta(I^i)$, i.e. a radio-frequency pulse applied selectively to the ith spin to "rotate" it through θ about the β axis of the rotating frame of reference. The condition to be satisfied here is

$$\theta = \gamma H_1 t_p, \tag{66}$$

where γ is the gyromagnetic ratio of the spin, H_1 is the strength of the magnetic field of the radio-frequency pulse, and t_p is the pulse duration time.

To implement $\exp[-i\phi I_z^i I_z^j]$, we make use of time evolution due solely to the spin-spin coupling between the ith and jth spins of the spin Hamiltonian [Eq. (18)], for a time period τ such that

$$\phi = 2\pi J_{ij}\tau\,, \tag{67}$$

where the effects of all other spin-spin couplings and all Zeeman evolutions are negated. To implement this type of time evolution, we make use of the property of a sequence [19,20]

$$(\pi)_x(I^i) - \frac{\tau}{2} - (\pi)_x(I^i)\,, \tag{68}$$

where $\tau/2$ is half of the evolution period. Its effect on the Zeeman evolution is given by

$$\exp[i\pi I_x^i]\,\exp[i\omega_0^i\frac{\tau}{2}I_z^i]\,\exp[i\pi I_x^i] = \exp[-i\omega_0^i\frac{\tau}{2}I_z^i]\,, \tag{69}$$

which tells that the direction of time evolution is now reversed. Therefore, this sequence, when preceded by another Zeeman evolution of a $\tau/2$ period, causes the cancellation of the evolution during the first $\tau/2$ period:

$$\Big(\exp[i\pi I_x^i]\,\exp[i\omega_0^i\frac{\tau}{2}I_z^i]\,\exp[i\pi I_x^i]\Big)\exp[i\omega_0^i\frac{\tau}{2}I_z^i] = 1\,. \tag{70}$$

Similarly, the effect of Eq. (68) on time evolution due to the spin-spin coupling is

$$\Big(\exp[i\pi I_x^i]\,\exp[-i2\pi J_{ij}\frac{\tau}{2}I_z^iI_z^j]\,\exp[i\pi I_x^i]\Big)\exp[-i2\pi J_{ij}\frac{\tau}{2}I_z^iI_z^j] = 1\,, \tag{71}$$

and, when the $(\pi)_x$ pulses are applied both to the ith and jth spins, time evolution due to the spin-spin coupling between this spin pair survives:

$$\Big(\exp[i\pi I_x^j]\,\exp[i\pi I_x^i]\,\exp[-i2\pi J_{ij}\frac{\tau}{2}I_z^iI_z^j]\,\exp[i\pi I_x^i]\,\exp[i\pi I_x^j]\Big)$$
$$\times\exp[-i2\pi J_{ij}\frac{\tau}{2}I_z^iI_z^j] = \exp[-i2\pi J_{ij}\tau I_z^iI_z^j]\,. \tag{72}$$

Using Eqs. (70), (71), and (72), we see that $\exp[-i\phi I_zS_z]$, for example, is implemented by the sequence

$$\frac{\tau}{2} - (\pi)_x(I,S) - \frac{\tau}{2} - (\pi)_x(I,S) \tag{73}$$

for the case of a two-spin system, and

$$\frac{\tau}{4} - (\pi)_x(K) - \frac{\tau}{4} - (\pi)_x(I,S,K) - \frac{\tau}{4} - (\pi)_x(K) - \frac{\tau}{4} - (\pi)_x(I,S,K)\,, \tag{74}$$

$$\frac{\tau}{8} - (\pi)_x(L) - \frac{\tau}{8} - (\pi)_x(K,L) - \frac{\tau}{8} - (\pi)_x(L) - \frac{\tau}{8} - (\pi)_x(I,S,K,L) - \frac{\tau}{8}$$
$$-(\pi)_x(L) - \frac{\tau}{8} - (\pi)_x(K,L) - \frac{\tau}{8} - (\pi)_x(L) - \frac{\tau}{8} - (\pi)_x(I,S,K,L) \tag{75}$$

for three- and four-spin systems, etc., where the evolution period τ is equal to $\phi/(2\pi J_{IS})$.

To summarize, since any f-controlled-NOT transformation U_f of any size is given by the product of spin exponential operators, and spin exponential operators of any size can be implemented in NMR, we can implement any U_f in NMR, without the help of an additional spin in the state $(|0\rangle - |1\rangle)/\sqrt{2}$ as used in Eq. (2).

[It has been shown [21] that a set of one-qubit rotations and two-qubit controlled-NOT transformations is the necessary and sufficient condition for a universal quantum computer. The latter transformation is defined by $CNOT: |x\rangle|y\rangle \longmapsto |x\rangle|y \oplus x\rangle$, which flips $(|0\rangle \leftrightarrow |1\rangle)$ the target qubit $|y\rangle$ if and only if the control qubit $|x\rangle$ is in the state $|1\rangle$. In NMR, a $CNOT(I,S)$ transformation where I and S are the control and the target spin, respectively, is given by $\exp[i(\pi/2)I_y]\ \exp[-i(\pi/2)I_x]\ \exp[-i(\pi/2)I_y]\ \exp[-i(\pi/2)S_x]\ \exp[i(\pi/2)S_y]\ \exp[-i\pi I_z S_z]\ \exp[-i(\pi/2)S_y]$ (up to the overall phase) [17]. Therefore, the ability to implement spin exponential operators in Eq. (65) leads to that an NMR quantum computer is universal.]

4. Discussion

The quantum nature of NMR computation as used in this work should be verified by the microscopic analog experiment [22] of the Greenberger-Horne-Zeilinger (GHZ) measurement [23,24]. To do this experiment, we use a four-spin system $ISKL$, and set up a maximally entangled GHZ state $|000\rangle - |111\rangle$ of the first three spins, and $|0\rangle$ of the fourth spin. Such state can be prepared from the "effective pure $|0000\rangle$ state," as follows [19]:

$$|0000\rangle \xrightarrow{H(I)} \xrightarrow{CNOT\,(I,S)} \xrightarrow{CCNOT\,(IS,K)} \frac{|000\rangle - |111\rangle}{\sqrt{2}^3}|0\rangle\,. \tag{76}$$

Here $H(I)$ is the Hadamard transformation on spin I, $CNOT(I,S)$ is the controlled-NOT transformation on S with I as the control, and $CCNOT(IS,K)$ is the controlled-controlled-NOT transformation on K with I and S as the controls; the last transformation flips spin K if and only if spins I and S are both in the state $|1\rangle$. [The GHZ state thus prepared from an "effective pure state" should not be confused with the GHZ state (which could be prepared from a pure state) [25], although the former transforms identically to the latter in NMR.] Notice here that the GHZ state is the eigenfunction of the operators $\sigma_x^I\sigma_y^S\sigma_y^K$, $\sigma_y^I\sigma_x^S\sigma_y^K$, $\sigma_y^I\sigma_y^S\sigma_x^K$, and $\sigma_x^I\sigma_x^S\sigma_x^K$, with respective eigenvalues $+1$, $+1$, $+1$, and -1, and that the relationship

$$(\sigma_x^I\sigma_x^S\sigma_x^K)\,(\sigma_y^I\sigma_y^S\sigma_x^K)\,(\sigma_y^I\sigma_x^S\sigma_y^K)\,(\sigma_x^I\sigma_y^S\sigma_y^K) = -1 \tag{77}$$

holds identically for any three-spin state [23,24].

In one type of the experiment [22], we correlate the state of spin L with the result that would be obtained if measurements were made of the polarizations of spins I, S, and K along different axes, and the results were multiplied together. For example, if we follow the three steps: (i) flip spin L if and only if spin I is in the state $|\downarrow_x\rangle$, (ii) flip spin L if and only if spin S is in the state $|\downarrow_y\rangle$, and (iii) flip spin L if and only if spin K is in the state $|\downarrow_y\rangle$, then spin L should be flipped an even number of times to result in the original state, corresponding to that the eigenvalue of $\sigma_x^I\sigma_y^S\sigma_y^K$ for the GHZ state being $+1$. Here, the step (i), for example, may be implemented [22] by: (a) first "rotating" spin I through $\pi/2$ about the y axis ($|\downarrow_x\rangle \rightarrow |\downarrow_z\rangle = |1\rangle$) by applying a $(\pi/2)_y(I)$ pulse,

(b) then applying a $CNOT(I, L)$ transformation, which flips spin L if and only if spin I is in the state $|1\rangle$, and (c) finally restoring spin I to its original state by a $(-\pi/2)_y(I)$ pulse. The GHZ state should remain intact after these operations, and be ready for the successive measurements of $\sigma_y^I \sigma_x^S \sigma_y^K$, etc.

The experimental success [26] to verify Eq. (77) (rather than that the right-hand side of this equation is $+1$) shows a contradiction to the existence of classical "hidden variables" for the spin operators as used in the NMR quantum computer experiments, and, therefore, the density operator I_x, which was prepared by "rotating" I_z through $-\pi/2$ about the y axis, should represent, not some classical state with an angular momentum along the x axis, but a polarization along the superpositions of the eigenstates, $|0\rangle$ and $|1\rangle$, of I_z:

$$I_x = \frac{1}{2}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\frac{\langle 0| + \langle 1|}{\sqrt{2}} - \frac{|0\rangle - |1\rangle}{\sqrt{2}}\frac{\langle 0| - \langle 1|}{\sqrt{2}}\right). \tag{78}$$

[A mixed state can be represented as a sum of pure states in infinitely many ways [24]. Equation (78) is one of the simplest representations of I_x.] This means that when we apply an f-controlled-NOT transformation $U_{f_{a_0 \cdots a_{N-1}}}$ [Eq. (26)] to our initial mixed state $\rho_{ini}^{(n)} = \sum_{i=1}^{n} I_x^i$ [Eq. (22)], we make use of quantum parallelism (i.e. the ability to manipulate superpositions) for an efficient manipulation of (the off-diagonal elements of) $\rho_{ini}^{(n)}$.

Mathematically, the problem to identify a given Boolean function as treated in this work belongs to the complexity class NP-complete (within the oracle model). A related problem to count the number of satisfying assignments to a given Boolean expression is also NP-complete, and NP-complete problems are known [27] to be reducible, in polynomial time, to the satisfiability (SAT) problem on Boolean expressions. It can be shown [6] that a mathematical model of a probabilistic ideal (i.e. infinite-size) ensemble computer for which the exact probabilities of each bit are available at the end of the computation is extremely powerful. For example, with such a computer, we can efficiently solve the assignment counting problem mentioned above; prepare the input in a uniformly random state, apply the expression P, and calculate the probability p that P is 1, then the answer is p times the number of possible inputs. Our NMR procedure to use an ensemble of bulk number of spins in the mixed state is a quantum mechanical implementation of such mathematical model (up to the noise present in any physical system); the uniformly random input is realized by the mixed state of polarizations along the superpositions, to which the f-controlled-NOT transformation is efficiently applied using quantum parallelism, and the exact probability of the output is certified by the ensemble averaging. Considering that even a probabilistic ensemble computer, which is the classical analogue of an ensemble quantum computer, can solve the assignment counting problem with an exponential speedup (within the bounded error model), the speedup we obtain by our NMR procedure in identifying a given Boolean function should basically due to the ensemble (rather than the quantum) nature of spins. It should, however, be noted that we cannot implement an exponentially efficient probabilistic ensemble computer without making use of quantum parallelism.

The ability of our procedure to solve the database searching problem with an exponential (rather than a square-root) speedup should tell that quantum procedures to use mixed states can be more powerful than "traditional" quantum procedures to use "ef-

fective pure states." Obviously, obstacles in the experiment, such as noise, decoherence, etc., are of the same order in magnitude for these types of procedures. Therefore it is concluded that a mixed-state NMR quantum computer, which is an implementation of the probabilistic ensemble computer to use quantum parallelism, is powerful enough to efficiently solve NP-complete problems, within the cost level of "traditional" quantum computers.

REFERENCES

1. D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985).
2. R. P. Feynman, Found. Phys. **16**, 507 (1986).
3. For a review, see *The Physics of Quantum Information : Quantum Cryptography, Quantum Teleportation, Quantum Computation*, edited by D. Bouwmeester, A. Ekert, and A. Zeilinger (Springer-Verlag, Berlin, 2000).
4. D. Deutsch and R. Jozsa, Proc. R. Soc. London, Ser. A **439**, 553 (1992).
5. N. A. Gershenfeld and I. L. Chuang, Science **275**, 350 (1997).
6. D. G. Cory, A. F. Fahmy, and T. F. Havel, Proc. Natl. Acad. Sci. USA **94**, 1634 (1997).
7. L. K. Grover, in *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing* (ACM Press, New York, 1996), pp. 212-218.
8. L. K. Grover, Phys. Rev. Lett. **79**, 325 (1997).
9. D. Collins, K. W. Kim, and W. C. Holton, Phys. Rev. A **58**, R1633 (1998).
10. M. Boyer, G. Brassard, P. Høyer, and A. Tapp, Fortsch. Phys. **46**, 493 (1998).
11. C. Zalka, Phys. Rev. A **60**, 2746 (1999).
12. D. Coppersmith, IBM Research Report RC19642 (1994).
13. R. R. Ernst, G. Bodenhausen, and A. Wokaun, *Principles of Nuclear Magnetic Resonance in One and Two Dimensions* (Clarendon Press, Oxford, 1991), Chap. 2.
14. D. G. Cory, M. D. Price, and T. F. Havel, Physica D **120**, 82 (1998).
15. U. Sakaguchi, H. Ozawa, and T. Fukumi, Phys. Rev. A **61**, 042313 (2000).
16. J. J. Sakurai, *Modern Quantum Mechanics* (Benjamin/Cummings, Menlo Park, CA, 1985), Chap. 3.
17. U. Sakaguchi, H. Ozawa, and T. Fukumi, NMR Quantum Computation, in *Coherence and Statistics of Photons and Atoms*, edited by J. Peřina (Wiley, New York, 2001), Sect. 11.2.
18. U. Sakaguchi, H. Ozawa, C. Amano, T. Fukumi, and W. S. Price, in *Mathematical Aspects of Quantum Information and Quantum Chaos*, edited by M. Ohya, RIMS Kokyuroku 1142 (Research Institute for Mathematical Sciences, Kyoto University, Kyoto, 2000), pp. 36-52.
19. U. Sakaguchi, H. Ozawa, C. Amano, and T. Fukumi, Phys. Rev. A **60**, 1906 (1999).
20. H. Ozawa, Phys. Rev. A **63**, 052312 (2001).
21. A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
22. S. Lloyd, Phys. Rev. A **57**, R1473 (1998).
23. N. D. Mermin, Am. J. Phys. **58**, 731 (1990).
24. A. Peres, *Quantum Theory : Concepts and Methods* (Kluwer Academic, Dordrecht, 1995), Chap. 6.
25. S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).
26. R. J. Nelson, D. G. Cory, and S. Lloyd, Phys. Rev. A **61**, 022106 (2000).
27. J. E. Hopcroft and J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation* (Addison-Wesley, Reading, MA, 1979), Chap. 13.